# Three-Day Awareness Programme On Cyber Security and Digital Forensics

**Organised by:**

**Cyber Forensic Research Centre, Department of Computer Science & Engineering,**
**Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur**
**In Collaboration with Gorakhpur Zone Police, Gorakhpur**

## Session(01) : Cyber Fraud Awareness and Prevention

**DAY(01): WEDNESDAY date: 21/10/2026**

Cybersecurity and digital forensics play a vital role in preventing cybercrime, protecting digital information, and supporting effective investigations. With the increasing use of digital technologies, awareness of cyber threats, online safety, digital evidence collection, and forensic investigation techniques has become increasingly important.

A Three-Day Awareness Programme on Cyber Security and Digital Forensics was organised to promote awareness of emerging cyber threats, cybercrime prevention, and the role of digital forensic technologies in modern investigations. The programme witnessed the participation of police officers from Gorakhpur Zone, who visited the Cyber Forensic Research Centre (CFRC), MMMUT, Gorakhpur, to gain insights into modern cybersecurity practices, digital forensic tools, and scientific methods used in cybercrime investigations.

As part of the programme, **Shri Upendra Kumar Singh, Sub-Inspector (SI), delivered an expert session on "Cyber Fraud Awareness and Prevention: Common Scams, Safety Measures, and Reporting Mechanisms."** The session focused on common cyber frauds, online scams, preventive measures, safe digital practices, and mechanisms for reporting cybercrime incidents.

The programme was graced by **Shri Arun Kumar S., ASP, Gorakhpur; Honourable Prof. Anupama Kaushik Sharma; Prof. Rakesh Kumar, Head, Department of Computer Science and Engineering; Dr. B. K. Sharma, Coordinator, CFRC Lab; and Dr. Vimal Kumar, Coordinator, CFRC Lab.** Their presence and valuable contributions highlighted the importance of collaboration between academic institutions and law enforcement agencies in strengthening cybersecurity awareness and digital forensic capabilities. The programme served as a valuable platform for knowledge sharing, practical learning, and promoting the effective use of digital forensic technologies in cybercrime investigations.

## COMMON TYPES OF CYBER FRAUD

The session highlighted common types of cyber fraud, including phishing, OTP scams, UPI fraud, fake calls, fraudulent links, and online financial scams. It focused on understanding how fraudsters deceive individuals and exploit their lack of awareness to obtain confidential information or financial details.

## PREVENTIVE MEASURES AND SAFE DIGITAL PRACTICES

The importance of protecting passwords and OTPs, avoiding suspicious links, verifying unknown callers, and exercising caution while making online payments was emphasised. Participants were encouraged to adopt safe digital practices and remain vigilant while using online services.

## CYBER FRAUD REPORTING MECHANISMS

The session highlighted the importance of promptly reporting cyber financial fraud through the National Cyber Crime Reporting Portal or helpline 1930. It also emphasised preserving relevant digital evidence, including transaction details, screenshots, and suspicious messages, to support the reporting and investigation process.

## CONCLUSION

The session highlighted the importance of cybersecurity awareness, preventive measures, and timely reporting in addressing cyber fraud. It reinforced the need for responsible digital behaviour and greater public awareness to promote a safer digital environment.


CYBER
SECURITY






CYBER
SECURITY



# Three-Day Awareness Programme On Cyber Security and Digital Forensics

**Organised by:**

**Cyber Forensic Research Centre, Department of Computer Science & Engineering,**
**Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur**
**In Collaboration with Gorakhpur Zone Police, Gorakhpur**

## Session(02) : Misuse of SIM Cards, Identity Documents, and Bank Accounts

**DAY(02): THURSDAY, date: 22/10/2026**

### INTRODUCTION

Cybercriminals may misuse personal identification documents, biometric authentication, SIM cards, and bank accounts to carry out fraudulent activities. Individuals who are unaware of these risks may unknowingly become involved in cybercrime. Awareness of identity protection, responsible use of banking services, and the safe handling of personal information is essential to preventing such incidents.

### SESSION OVERVIEW

As part of the Cyber Security and Digital Forensics Awareness Programme, police personnel from the Cyber Crime Branch, Gorakhpur, conducted an awareness session on the misuse of SIM cards, identity documents, and bank accounts in cyber fraud. The session highlighted how fraudsters exploit people's trust, financial difficulties, and lack of awareness to obtain access to personal information and financial services for illegal activities.

### MISUSE OF SIM CARDS AND BIOMETRIC AUTHENTICATION

The session explained how fraudsters may misuse an individual's identity documents and biometric authentication to obtain multiple SIM cards. Such SIM cards may subsequently be used for fraudulent calls, deceptive messages, and other cybercriminal activities. Individuals were advised to remain cautious during SIM card registration, verify the purpose of biometric authentication, and ensure that their identity is used only for authorised purposes.

### MISUSE OF IDENTITY DOCUMENTS

The police personnel highlighted how fraudsters may offer money or other benefits in exchange for personal documents, taking advantage of individuals who may not fully understand the consequences. These documents may be misused to obtain SIM cards, open accounts, or facilitate other fraudulent activities without the individual's informed

understanding. Participants were advised not to share identity documents with unknown or unauthorised persons and to verify the legitimacy of any request for personal information.

**MISUSE OF BANK ACCOUNTS IN CYBER FRAUD**

The session also explained how individuals may be persuaded to provide access to their bank accounts in exchange for money or other incentives. Fraudsters may use these accounts to receive, transfer, or withdraw money obtained through cybercrime. Individuals whose accounts are used in this manner may face financial losses, account restrictions, and potential legal consequences, even if they claim not to have known the source of the funds.

Participants were cautioned never to allow others to use their bank accounts for unknown transactions or share their banking credentials, PINs, passwords, or OTPs with anyone.

**PREVENTIVE MEASURES AND SAFETY AWARENESS**

The session emphasised the importance of protecting personal identification documents, using biometric authentication carefully, and obtaining SIM cards only through authorised channels. Participants were encouraged to monitor their bank transactions regularly, avoid accepting money in exchange for the use of their bank accounts, and immediately contact their bank if they notice suspicious transactions. Responsible handling of personal and financial information can help reduce the risk of identity theft and cyber fraud.

**REPORTING AND LEGAL AWARENESS**

The importance of promptly reporting suspected cyber fraud to the appropriate authorities was highlighted. Individuals who experience financial cyber fraud can contact the national cybercrime helpline at **1930** or submit a complaint through the National Cyber Crime Reporting Portal. Relevant records, including transaction details, messages, and other available evidence, should be preserved to assist the investigation.

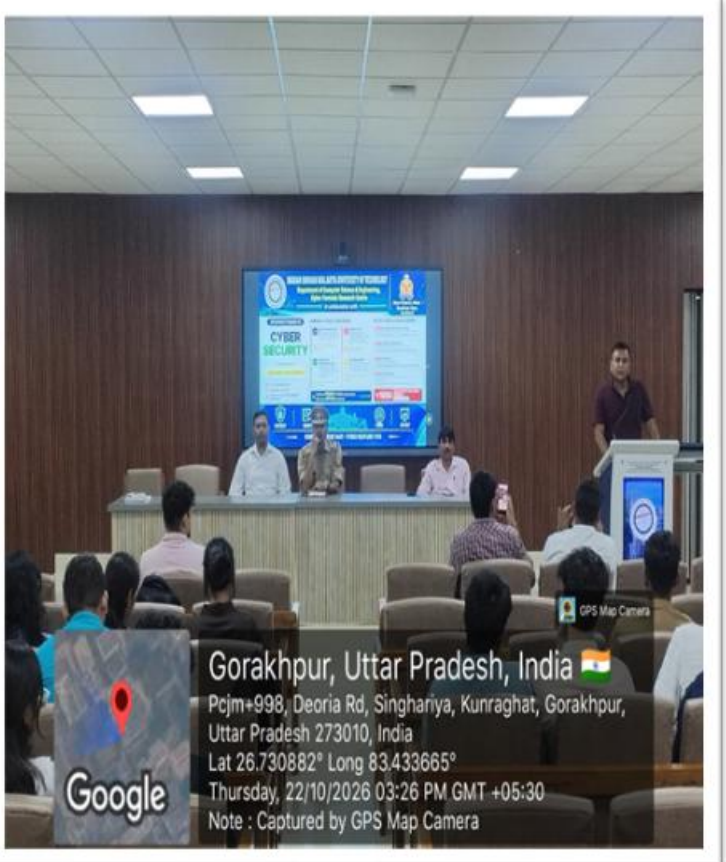
The session also raised awareness that knowingly facilitating fraudulent transactions or allowing bank accounts to be used for illegal activities can have serious legal consequences.

**CONCLUSION**

The session highlighted the risks associated with the misuse of SIM cards, biometric authentication, personal identity documents, and bank accounts in cyber fraud. It emphasised the importance of protecting personal information, verifying the purpose of authentication requests, and refusing offers that involve sharing identity documents or bank account access in exchange for money. The awareness session reinforced the need for responsible financial practices, vigilance, and timely reporting to help prevent cybercrime

and protect individuals from becoming victims or unwitting participants in fraudulent activities.





# Three-Day Awareness Programme On Cyber Security and Digital Forensics

**Organised by:**

**Cyber Forensic Research Centre, Department of Computer Science & Engineering,**
**Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur**
**In Collaboration with Gorakhpur Zone Police, Gorakhpur**

## Session(03) : Cyber Fraud Through Fraudulent Overseas Job and Placement Offers

**DAY(02): THURSDAY, date: 22/10/2026**

### INTRODUCTION

Fraudulent overseas job offers and placement opportunities have emerged as a serious concern, particularly for young people seeking employment abroad. Cybercriminals may exploit students' aspirations for international careers by offering attractive salaries, promising placements, and misleading employment opportunities. In some cases, individuals are taken to foreign countries under false pretences and subsequently forced or coerced into participating in cyber fraud activities.

### AWARENESS SESSION BY CYBER CELL, GORAKHPUR

During the session, police personnel from the Cyber Cell, Gorakhpur, explained how fraudulent recruitment networks may target students and job seekers through fake placement offers and promises of employment in foreign countries. Such individuals may be misled about the actual nature of the job and the activities they will be expected to perform after reaching their destination.

### MISUSE OF STUDENTS THROUGH FRAUDULENT RECRUITMENT

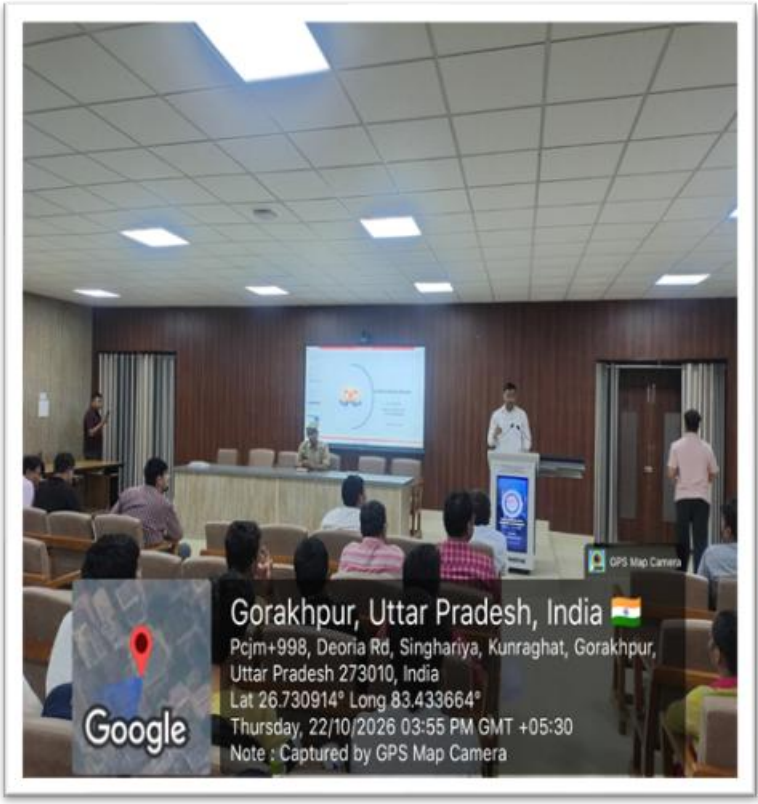
The session highlighted how some criminal networks lure young people with promises of attractive salaries, overseas employment, and better career opportunities. After reaching a foreign country, victims may discover that the work differs significantly from what was promised. In certain cases, they may be pressured, threatened, or forced to participate in cyber fraud operations targeting people through online scams and other fraudulent activities.

### PREVENTIVE MEASURES AND STUDENT AWARENESS

The police personnel emphasised the importance of verifying overseas job offers, recruitment agencies, employment contracts, and the legitimacy of prospective employers before accepting any placement. Students were advised to remain cautious of unrealistic salary offers, avoid handing over passports or personal documents to unauthorised persons, and seek verification through appropriate official channels before travelling abroad for employment.

**CONCLUSION**

The session raised awareness about the risks associated with fraudulent overseas placement offers and the exploitation of young people by organised cybercrime networks. It highlighted the importance of verifying employment opportunities, understanding the nature of the proposed work, and exercising caution before accepting overseas job offers. The session reinforced the need for greater awareness among students and job seekers to prevent exploitation and reduce the risk of becoming involved in cybercrime.







GPS Map Camera
Gorakhpur, Uttar Pradesh, India
Pcjm+998, Deoria Rd, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730919° Long 83.433663°
Thursday, 22/10/2026 03:55 PM GMT +05:30
Note : Captured by GPS Map Camera
Google



# Three-Day Awareness Programme On Cyber Security and Digital Forensics

**Organised by:**

**Cyber Forensic Research Centre, Department of Computer Science & Engineering,**
**Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur**
**In Collaboration with Gorakhpur Zone Police, Gorakhpur**

## Session (04): Cybercrime Awareness, Online Safety, And Preventive Measures

**DAY(03): FRIDAY, date: 23/10/2026**

### INTRODUCTION

Cybercrime awareness plays an important role in protecting individuals from online threats and digital fraud. With the increasing use of the internet, smartphones, social media platforms, and digital payment services, people may face various cyber risks. Awareness of common cyber threats, safe online practices, and preventive measures is essential for protecting personal information and ensuring digital security.

### SESSION OVERVIEW

During the session, personnel from the Cyber Crime Branch, Gorakhpur, provided awareness about cybercrime, online safety, and the importance of responsible digital behaviour. The session focused on helping participants understand common cyber threats, recognise suspicious online activities, and adopt appropriate safety measures while using digital platforms and internet-based services.

### COMMON TYPES OF CYBERCRIME

The session highlighted different forms of cybercrime, including online financial fraud, phishing, identity theft, fake social media profiles, fraudulent links, and online scams. Participants were made aware that cybercriminals may use deceptive messages, phone calls, fake websites, and misleading offers to obtain personal information or access financial accounts. The importance of remaining alert while interacting with unknown individuals and online platforms was emphasised.

### ONLINE SAFETY AND DIGITAL SECURITY

The importance of maintaining online safety while using social media, internet banking, and digital payment applications was discussed. Participants were advised to use strong and unique passwords, avoid sharing One-Time Passwords (OTPs), PINs, and banking credentials, and refrain from clicking suspicious links. They were also encouraged to verify the authenticity of websites, messages, and online offers before sharing personal or financial information.

**PREVENTIVE MEASURES AND SAFETY AWARENESS**

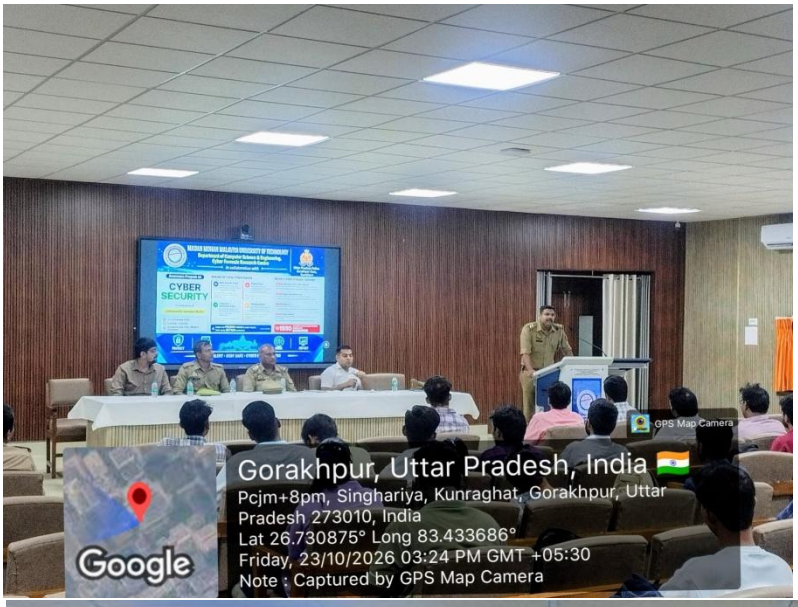
The session emphasised the importance of adopting preventive measures to reduce the risk of cybercrime. Participants were encouraged to keep their devices and applications updated, use appropriate security settings, avoid downloading files from untrusted sources, and exercise caution when connecting to public Wi-Fi networks. They were also advised to report suspicious activities promptly and preserve relevant digital evidence, such as messages, screenshots, and transaction details, whenever required.

CYBERCRIME REPORTING AND LEGAL AWARENESS

The importance of reporting cybercrime incidents to the appropriate authorities was highlighted. Participants were informed that financial cyber fraud can be reported through the national cybercrime helpline 1930 or the official National Cyber Crime Reporting Portal. Prompt reporting and the preservation of relevant evidence can help authorities investigate incidents and take appropriate action.

**CONCLUSION**

The session enhanced awareness of cybercrime risks, online safety practices, and preventive measures. It highlighted the importance of responsible internet usage, protection of personal and financial information, and timely reporting of suspicious activities. The session reinforced the need for digital awareness and vigilance to help individuals protect themselves against cyber threats.


CYBER SECURITY
GPS Map Camera
Gorakhpur, Uttar Pradesh, India
Pcjm+8pm, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730875° Long 83.433686°
Friday, 23/10/2026 03:24 PM GMT +05:30
Note : Captured by GPS Map Camera
Google


CYBER SECURITY


CYBER SECURITY
GPS Map Camera
Gorakhpur, Uttar Pradesh, India
Pcjm+998, Deoria Rd, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730884° Long 83.433692°
Friday, 23/10/2026 03:24 PM GMT +05:30
Note : Captured by GPS Map Camera
Google

# Three-Day Awareness Programme On Cyber Security and Digital Forensics

**Organised by:**

**Cyber Forensic Research Centre, Department of Computer Science & Engineering,**
**Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur**
**In Collaboration with Gorakhpur Zone Police, Gorakhpur**

Session (05): Digital Evidence, Cybercrime Investigation, and Reporting Procedures

**DAY(03): FRIDAY, date: 23/10/2026**

## INTRODUCTION

Digital evidence plays an important role in the investigation of cybercrime and other offences involving electronic devices. Information stored on mobile phones, computers, storage devices, social media platforms, and digital communication systems can help investigators understand incidents and establish relevant facts. The proper identification, collection, preservation, and examination of digital evidence are essential for supporting investigations.

## SESSION OVERVIEW

The session focused on the importance of digital evidence in cybercrime investigations and the procedures involved in reporting cyber-related incidents. It highlighted how electronic information can assist investigating authorities in understanding the nature of an incident, identifying relevant digital traces, and supporting the investigation process. The importance of handling digital evidence carefully and responsibly was also emphasised.

## IMPORTANCE OF DIGITAL EVIDENCE

Digital evidence may include emails, text messages, call records, photographs, videos, internet activity records, social media communications, and online financial transaction details. Such information can help investigators understand the sequence of events and identify connections between individuals, devices, and online activities. Participants were made aware that digital evidence must be handled carefully to avoid accidental alteration, loss, or destruction.

## COLLECTION AND PRESERVATION OF DIGITAL EVIDENCE

The session highlighted the importance of preserving relevant information when a cybercrime incident occurs. Individuals should retain available screenshots, messages, emails, transaction IDs, relevant phone numbers, and other supporting records. Electronic

devices and original data should not be unnecessarily modified or deleted. In formal investigations, authorised personnel should follow appropriate forensic procedures to maintain the integrity and authenticity of digital evidence.

**ROLE OF DIGITAL FORENSICS IN CYBERCRIME INVESTIGATION**

Digital forensics supports cybercrime investigations through the systematic examination of electronic devices and digital information. Forensic techniques may help investigators recover relevant data, examine digital activity, analyse communication records, and identify information connected with an incident. The examination should be conducted using appropriate tools and established procedures so that findings can be documented accurately and used for investigative purposes.

**CYBERCRIME REPORTING PROCEDURES**

The importance of reporting cybercrime incidents promptly to the appropriate authorities was discussed. In cases of financial cyber fraud, individuals in India can contact the national cybercrime helpline at **1930** or submit a complaint through the National Cyber Crime Reporting Portal. While reporting an incident, individuals should provide accurate information and preserve relevant supporting records, such as transaction details, screenshots, messages, and suspicious contact information.

**CONCLUSION**

The session highlighted the importance of digital evidence, forensic examination, and proper reporting procedures in cybercrime investigations. It reinforced the need to preserve relevant electronic information, handle digital evidence responsibly, and report cybercrime incidents without unnecessary delay. The session contributed to a better understanding of how digital evidence and forensic practices support effective cybercrime investigation.






# Three-Day Awareness Programme On Cyber Security and Digital Forensics

**Organised by:**

**Cyber Forensic Research Centre, Department of Computer Science & Engineering,**
**Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur**
**In Collaboration with Gorakhpur Zone Police, Gorakhpur**

## Session (06): Social Media Security, Cyberbullying, and Online Harassment

**DAY(03): FRIDAY, date: 23/10/2026**

### INTRODUCTION

Social media has become an important part of daily life, enabling people to communicate, share information, and connect with others. However, the misuse of social media platforms can lead to various cyber threats, including fake profiles, identity theft, cyberbullying, online harassment, and privacy violations. Awareness of these risks and the adoption of appropriate security measures are essential for maintaining a safe digital environment.

### SESSION OVERVIEW

During the session, personnel from the Cyber Crime Branch, Gorakhpur, discussed the importance of social media security and awareness of online threats. The session focused on identifying suspicious online activities, understanding the risks associated with sharing personal information, and recognising different forms of cyberbullying and online harassment. Participants were encouraged to use social media responsibly and follow appropriate digital safety practices.

### SOCIAL MEDIA SECURITY AND PRIVACY

The session highlighted the importance of protecting personal information while using social media platforms. Users were advised to maintain strong passwords, enable two-factor authentication wherever available, review account privacy settings, and avoid accepting requests from unknown or suspicious profiles. Participants were also made aware of the risks associated with sharing sensitive personal information, photographs, location details, and other private content publicly.

### CYBERBULLYING AND ONLINE HARASSMENT

Cyberbullying and online harassment involve the misuse of digital platforms to threaten, intimidate, embarrass, or repeatedly target individuals. Such activities may include abusive messages, threatening comments, spreading false information, impersonation, and the

unauthorised sharing of personal photographs or information. The session emphasised the importance of recognising such behaviour, avoiding engagement with abusive accounts, and seeking assistance from trusted individuals or appropriate authorities when nec essary.

**FAKE PROFILES AND ONLINE IMPERSONATION**

The session addressed the risks associated with fake social media profiles and online impersonation. Fraudsters may create accounts using another person's name, photographs, or personal information to mislead others, damage reputations, or carry out fraudulent activities. Participants were advised to verify suspicious profiles, avoid sharing confidential information with unknown individuals, and report fake accounts through the relevant platform's reporting mechanism.

**PREVENTIVE MEASURES AND REPORTING**

Participants were encouraged to use strong and unique passwords, enable available security features, and regularly review their social media privacy settings. In cases of cyberbullying or online harassment, individuals should preserve relevant evidence, such as screenshots, profile links, messages, and timestamps. They should report abusive accounts to the concerned platform and contact the appropriate authorities when necessary. Cybercrime complaints in India can also be submitted through the National Cyber Crime Reporting Portal.

**CONCLUSION**

The session highlighted the importance of social media security, online privacy, and responsible digital behaviour. It raised awareness of the risks associated with cyberbullying, fake profiles, identity misuse, and online harassment. The session reinforced the need to protect personal information, recognise suspicious activities, preserve relevant evidence, and report cybercrime incidents promptly to promote a safer online environment.




MADAN MOHAN MALAVIYA UNIVERSITY OF TECHNOLOGY
Department of Computer Science & Engineering,
Cyber Forensic Research Centre
CYBER
SECURITY


MADAN MOHAN MALAVIYA UNIVERSITY OF TECHNOLOGY
Department of Computer Science & Engineering,
Cyber Forensic Research Centre
CYBER
SECURITY




CYBER
SECURITY


CYBER
SECURITY